*Tu*

# UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/748,538 | 12/29/2003 | Kevin H. Embree | 2043.046US1 | 8540 |

49845          7590          12/13/2007
SCHWEGMAN, LUNDBERG & WOESSNER/EBAY
P.O. BOX 2938
MINNEAPOLIS, MN 55402

| EXAMINER |
|---|
| TURNER, ASHLEY D |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2154 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 12/13/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@SLWIP.COM

PTOL-90A (Rev. 04/07)

| | | Application No. | Applicant(s) |
|---|---|---|---|
| **Office Action Summary** | | 10/748,538 | EMBREE ET AL. |
| | | Examiner | Art Unit | |
| | | Ashley D. Turner | 2154 | |

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after t he mailing date of this communication, even if timely filed, may re duce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on _29 December 2003_.
2a) ☐ This action is **FINAL**.     2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) _1-38_ is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _1-38_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some *   c) ☐ None of:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____.
    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

# DETAILED ACTION

## *Claim Rejections - 35 USC § 101*

1.      35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims1- 18 and 38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non- statutory subject matter.

Independent claim 1 is drawn towards a apparatus to process issue data pertaining to a system, the apparatus including: a prioritization engine to receive issue data from a reporting entity via a network, the issue data reporting an issue pertaining to the system and including an identifier to identify the reporting entity; and a user performance module to access a database, and utilizing the identifier, to retrieve performance data regarding the reporting entity from a database, the performance data indicative of a past performance of the reporting entity in reporting issues pertaining to the system; the prioritization engine automatically to prioritize a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity.  Regarding claim 1 the claim is drawn toward software per se as evident in the specification on page 9 [0014] " The various marketplace and payment applications 30 and 32 could also be

implemented as standalone software programs, which do not necessarily have networking capabilities".

Claim 2-18 are rejected for the same reasoning as described above.

Independent claim 1 is drawn towards a machine –readable medium and storing a sense of instructions that, when executed by a machine, cause the machine to: receive issue data from a reporting entity, the issue data reporting an issue pertaining to the system and including an identifier to identify the reporting entity; utilize the identifier, accessing a database to retrieve performance data regarding the reporting entity, the performance data indicative of a past performance of the reporting entity in reporting issues pertaining to the system; and automatically prioritized a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity. Base on 35 U.S.C.101, the Supreme Court has specifically identified three categories of statutory subject matter: which are a machine, manufacture, composition of matter, and a process. In the instant case, applicant recitation on page 36, section [0093] "The term "machine-readable medium" shall accordingly be taken to include, but not limited to, solid-state memories, optical and magnetic media, and carrier wave signals. Furthermore, carrier waves that pass through the air are in non-statutory category, it's factual that the claims lack the physical medium necessary to produce a tangible output result.

## *Claim Rejections - 35 USC § 112*

3. Claim 38 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which   applicant

regards as the invention.

Regarding claim 38 line 1 the phrase "A machine –readable medium and storing a

sense of instructions" is unclear. The metes and bounds of the claim cannot be

determined.

## *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1,7,8,11,12,14,18,19,25,26,29,30,32,36,37,38 are rejected under 35 U.S.C. 103

(a) as being unpatentable over Witter (US 2003/0208497 A1) in view of Masters (US

7,051,098 B2).

As per claim 1 Witter discloses an apparatus to process issue data pertaining to a

system, the apparatus including: a prioritization engine to receive issue data from a

reporting entity via a network, the issue data reporting an issue pertaining to the system

and including an identifier to identify the reporting entity; and a user performance

module to access a database, and utilizing the identifier, to retrieve performance data

regarding the reporting entity from a database, the performance data indicative of a past

performance of the reporting entity in reporting issues pertaining to the system

(Abstract); Witter did not disclose the prioritization engine automatically to prioritize a

response activity, responsive to the issue, utilizing the performance data regarding the

reporting entity. The general concept of the prioritization engine automatically to

prioritize a response activity, responsive to the issue, utilizing the performance data

regarding the reporting entity is well known in the art as taught by Masters. Masters

discloses the prioritization engine automatically to prioritize a response activity,

responsive to the issue, utilizing the performance data regarding the reporting entity

(Col.7 Fig.1 lines 35-45 Col.8 lines 10-34). It would have been obvious to one of

ordinary skill in the art at the time of the invention to modify Witter to include the

prioritization engine automatically to prioritize a response activity, responsive to the

issue, utilizing the performance data regarding the reporting entity in order to have a

user –friendly technique with which specify quality of service requirements for each

host, each application, and the network in which the hosts are connected.

As per claim 7 Witter and Masters discloses all the limitations of claim 7 which is

described above. Master also discloses the prioritization engine is to communicate the

issue data to an agent for performance of the response activity, the communicating of

the issue data to the agent being performed according to a priority assigned to the issue

(Col. 32 lines 33-47).

As per claim 8 Witter and Masters discloses all the limitations of claim 8 which is

described above. Masters also discloses the agent is to assess the validity of the issue,

and to cause of the updating of the performance data regarding the reporting entity

based on the assessed validity of the issue (Col. 26 lines 12-28).

As per claim 11 Witter and Masters discloses all the limitations of claim 11 which is

described above. Masters also discloses wherein the prioritization engine is to identify

an issue type for the issue and to retrieve the predetermined severity value utilizing the

identified issue type (Col. 31 lines 45-55) (Col. 33 lines 60-67).

As per claim 12 Witter and Masters discloses all the limitation of claim 12 which is

described above. Master also discloses wherein the prioritization engine is to identify an

issue type for the issue and to retrieve the predetermined severity value utilizing the

identified issue type (Col. 31 lines 45-55) (Col. 33 lines 60-67).

As per claim 14 Witter and Masters discloses all the limitations of claim 14 which is

described above. Witter also discloses wherein the prioritization engine is to prioritize

the response activity utilizing a combination of at least two of the performance data, a

count of a number of times that the issue has been reported, a predetermined severity

value associated with the issue, and exposure information associated with the issue

(Col. 31 lines 45-55) (Col. 33 lines 60-67).

As per claim 18 Witter and Master disclose all the limitations of claim 18 which is

described above. Masters also discloses wherein the user performance module is

selectively to present an issue data report mechanism based on the performance data

indicative of the past performance of the reporting entity (Abstract) (Paragraph [0066]).

As per claim 19 Witter discloses a computer- implemented method to process issue

data pertaining to a system, the method including: receiving issue data from a reporting

entity, the issue data reporting an issue pertaining to the system and including an

identifier to identify the reporting entity, utilizing the identifier, accessing a database to

retrieve performance data regarding the reporting entity, the performance data

indicative of a past performance of the reporting entity in reporting issues pertaining to

the system (Abstract). Witter did not disclose automatically prioritizing a response

activity, responsive to the issue, utilizing the performance data regarding the reporting

entity. The general concept of automatically prioritizing a response activity, responsive

to the issue, utilizing the performance data regarding the reporting entity is well known

in the art as taught by Masters. Masters discloses automatically prioritizing a response

activity, responsive to the issue, utilizing the performance data regarding the reporting

entity (Col.7 Fig.1 lines 35-45 Col.8 lines 10-34). It would have been obvious to one of

ordinary skill in the art at the time of the invention to modify Witter to include the

prioritization engine automatically to prioritize a response activity, responsive to the

issue, utilizing the performance data regarding the reporting entity in order to have a

user –friendly technique with which specify quality of service requirements for each

host, each application, and the network in which the hosts are connected.

As per claim 25 Witter and Masters discloses all the limitations of claim 25 which are

described above. Masters also discloses communicating the issue data to an agent for

performance of the response activity, the communicating of the issue data to the agent

begin performed according to a priority assigned to the issue (Col. 32 lines 33-47).

As per claim 26 Witter and Masters discloses all the limitations of claim 26 which are

described above. Masters also discloses the agent is to assess the validity of the issue,

and to cause of the updating of the performance data regarding the reporting entity

based on the assessed validity of the issue (Col. 26 lines 12-28).

As per claim 29 Witter and Masters discloses all the limitations of claim 29 which are

described above. Masters also discloses retrieving a predetermined severity value

associated with the issue, and prioritizing the response activity utilizing the

predetermined severity value (Col. 31 lines 45-55) (Col. 33 lines 60-67).

As per claim 30 Witter and Masters discloses all the limitation of claim 30 which is

described above. Master also discloses identifying an issue type for the issue, and

retrieving the predetermined severity value utilizing the identified issue type (Col. 31

lines 45-55) (Col. 33 lines 60-67).

As per claim 32 Witter and Masters discloses all the limitation of claim 32 which is

described above. Master also discloses prioritizing the response activity utilizing a

combination of at least two of the performance data, a count of a number of times that

the issue has been reported, a predetermined severity value associated with the issue,

and exposure information associated with the issue (Col. 31 lines 45-55) (Col. 33 lines

60-67).

As per claim 36 Witter and Master disclose all the limitations of claim 36 which is

described above. Masters also discloses including selectivity presenting an issue data

report mechanism based on the performance data indicative of the past performance of

reporting entity. (Abstract) (Paragraph [0066]).

As per claim 37 Witter discloses an apparatus to process issue data pertaining to a

system, the apparatus including prioritization means for receiving issue data from a

reporting entity via a network, the issue data reporting an issue pertaining to the system

and including an identifier to identify the reporting entity (Abstract); and performance

means to access a database, and utilizing the identifier, to retrieve performance data

regarding the reporting entity from a database, the performance data indicative of a past

performance of entity in reporting issue pertaining to the system(Abstract); Witter did not

disclose the prioritization means automatically for prioritizing a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity. The general concept of the prioritization means automatically for prioritizing a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity is well known in the art as taught by Masters. Masters discloses the prioritization means automatically for prioritizing a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity (Col.7 Fig.1 lines 35-45 Col.8 lines 10-34). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Witter to include prioritization means automatically for prioritizing a response activity, responsive to the issue, utilizing the performance data regarding the reporting entity in order to have a user –friendly technique with which specify quality of service requirements for each host, each application, and the network in which the hosts are connected.

As per claim 38 Witter discloses a machine-readable medium and storing a sense of instructions that, when executed by a machine, cause the machine to receive issue data from a reporting entity, the issue data reporting an issue pertaining to the system and including an identifier to identify the reporting entity; utilize the identifier, accessing a database to retrieve performance data regarding the reporting entity, the performance data indicative of a past performance of the reporting entity in reporting issues pertaining to the system (Abstract). Witter did not disclose automatically prioritized a response activity, responsive to the issue, utilizing the performance data regarding the

reporting entity. The general concept of automatically prioritized a response activity,

responsive to the issue, utilizing the performance data regarding the reporting entity is

well known in the art as disclosed by Masters. Masters discloses automatically

prioritized a response activity, responsive to the issue, utilizing the performance data

regarding the reporting entity (Col.7 Fig.1 lines 35-45 Col.8 lines 10-34). It would have

been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include automatically prioritized a response activity, responsive to the issue,

utilizing the performance data regarding the reporting entity in order to have a user –

friendly technique with which specify quality of service requirements for each host, each

application, and the network in which the hosts are connected.


Claims 2-6,13,20-24,31 are rejected under 35 U.S.C. 103 (a) as being unpatentable

over Witter (US 2003/0208497 A1) in view of Masters (US 7,051,098 B2) further in view

of Khanolkar (US 2007/0234426 A1).


As per claim 2 Witter and Masters discloses all the limitations of claim 2 which are

described above. Witter did not disclose wherein the performance data indicates a

historical accuracy with which the reporting entity has previously reported issues

pertaining to the system. The general concept of wherein the performance data

indicates a historical accuracy with which the reporting entity has previously reported

issues pertaining to the system is well known in the art as taught by Khanolkar.

Khanolkar discloses wherein the performance data indicates a historical accuracy with

which the reporting entity has previously reported issues pertaining to the system

(Khanolkar: Pg. 1 [0004] Presented with log data, however, monitoring devices often

fail in two respects. First, they fail to effectively monitor log data from all relevant

components on the network. Second, they fail to record and report the log data in a form

that is timely and useful to network administrators. Moreover, while various systems

such as firewalls and intrusion detection systems, such as NetRanger from Cisco

Systems, Inc., may issue real time alarms to a network administrator of an intrusion

event based on log data; within a network such alarms may be lost in the midst of

numerous notices of intrusion events received by a network administrator. What is

needed is a system to process and organize network intrusion events and log data from

a number of network systems and provide them to a user in an interface that

summarizes them, yet has links to more detailed information, that provides for real time

notice and communications regarding current events, and that allows for the compilation

and recalling of past log data and intrusion events for detection of patterns of activity for

later use and consultation). It would have been obvious to one of ordinary skill in the art

at the time of the invention to modify Witter in order to include wherein the performance

data indicates a historical accuracy with which the reporting entity has previously

reported issues pertaining to the system in order to provide access to the corresponding

event object information via an alarm console.


As per claim 3 Witter and Masters discloses all the limitations of claim 3 which are

described above. Witter did not disclose wherein the historical accuracy is expressed in

terms of a number of false positive issue data received from the reporting entity. The

general concept of wherein the historical accuracy is expressed in terms of a number of

false positive issue data received from the reporting entity is well known in the art as

taught by Khanolkar. Khanolkar discloses the historical accuracy is expressed in terms

of a number of false positive issue data i.e. event object received from the reporting

entity (Khanolar: Each event object that is created is read, and the intrusion event

information it contains is assigned a severity level. Event objects meeting or exceeding

a predetermined threshold security level, or other threshold criteria, may be broadcast

to the user and displayed as an intrusion alarm on a user interface display screen in real

time. Users may set filters regulating the stream of event objects received as

broadcasts based on severity level or other criteria or may choose to receive all event

objects regardless of severity or other criteria as broadcast intrusion alarms). It would

have been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include the historical accuracy is expressed in terms of a number of false

positive issue data received from the reporting entity in order to provide access to the

corresponding event object information via an alarm console.

As per claim 4 Witter and Masters discloses all the limitations of claim 4 which are

described above. Masters did not disclose wherein the performance data indicates a

rate at which the reporting entity has previously reported issues pertaining to the

system. The general concept of the performance data indicates a rate at which the

reporting entity has previously reported issues pertaining to the system is well known in

the art as taught by Khanolakor. Khanolakor discloses the performance data indicates a

rate at which the reporting entity has previously reported issues pertaining to the system

(Khanolakor: Pg. 1 [0006] In response to an intrusion event, the security monitoring

system can issue intrusion alarms to network administrative users ("users"), who will

then be able to obtain information regarding intrusion events in real time on a display

screen. The system filters log data, which contains information related to intrusion

events, to provide a more manageable flow of data that can be more easily reviewed by

a system administrator because the data relating to intrusion events are not "lost" in

large amounts of noise (e.g., data not relating to intrusion events). The system has

means for organizing and collating intrusion event data within a searchable database

accessible to a user through a reporting system that can generate security reports and

summaries of intrusion events for network service devices and that provides information

in response to user queries). It would have been obvious to one of ordinary skill in the

art at the time of the invention to modify Witter to include the performance data indicates

a rate at which the reporting entity has previously reported issues pertaining to the

system in order to provide access to the corresponding event object information via an

alarm console.

As per claim 5 Witter and Masters discloses all the limitations of claim 5 which are

described above. Master did not disclose the user performance module is to assess

validity of the issue pertaining to the system as reported in the issue data, and to update

the performance data regarding the reporting entity based on the assessed validity of

the issue. The general concept of the user performance module is to assess validity of

the issue pertaining to the system as reported in the issue data, and to update the

performance data regarding the reporting entity based on the assessed validity of the

issue is well known in the art as taught by Khanolakor. Khanolakor discloses the user

performance module is to assess validity of the issue pertaining to the system as

reported in the issue data, and to update the performance data regarding the reporting

entity based on the assessed validity of the issue (Pg. 1 [0008] Each event object that is

created is read, and the intrusion event information it contains is assigned a severity

level. Event objects meeting or exceeding a predetermined threshold security level, or

other threshold criteria, may be broadcast to the user and displayed as an intrusion

alarm on a user interface display screen in real time. Users may set filters regulating the

stream of event objects received as broadcasts based on severity level or other criteria

or may choose to receive all event objects regardless of severity or other criteria as

broadcast intrusion alarms). It would have been obvious to one of ordinary skill in the art

at the time of the invention to modify Witter to include the user performance module is to

assess validity of the issue pertaining to the system as reported in the issue data, and to

update the performance data regarding the reporting entity based on the assessed

validity of the issue in order to provide access to the corresponding event object

information via an alarm console.

As per claim 6 Witter and Masters disclose all the limitations of claim 6 which are described above. Master did not disclose the user performance module is to update the performance data by registering at least one of a false positive and a false negative with respect issue. The general concept of the user performance module is to update the performance data by registering at least one of a false positive and a false negative with respect issue is well known in the art as taught by Khanolakar. Khanolar discloses the user performance module is to update the performance data by registering at least one of a false positive and a false negative with respect issue (Pg. 3 [0004] Logging is the procedure by which operating systems record events in the system as they happen. Within the logging memory of these devices, and other devices such as web servers, e-mail servers, DNS servers, etc., logs are kept that contain data comprising information chronicling network intrusion events. Presented with log data, however, monitoring devices often fail in two respects. First, they fail to effectively monitor log data from all relevant components on the network. Second, they fail to record and report the log data in a form that is timely and useful to network administrators. Moreover, while various systems such as firewalls and intrusion detection systems, such as NetRanger from Cisco Systems, Inc., may issue real time alarms to a network administrator of an intrusion event based on log data; within a network such alarms may be lost in the midst of numerous notices of intrusion events received by a network administrator. What is needed is a system to process and organize network intrusion events and log data from a number of network systems and provide them to a user in an interface that summarizes them, yet has links to more detailed information, that provides for real time

notice and communications regarding current events, and that allows for the compilation

and recalling of past log data and intrusion events for detection of patterns of activity for

later use and consultation). It would have been obvious to one of ordinary skill in the art

at the time of the invention to modify Witter in order to provide access to the

corresponding event object information via an alarm console.


As per claim 13 Witter and Masters discloses all the limitation of claim 13 which is

described above. Witter did not disclose wherein the prioritization engine is retrieve

predetermined exposure information associated with the issue, and to prioritize the

response activity utilizing the predetermined exposure information, predetermined

exposure information indicating at east one of a loss and liability value attributed to the

issue. The general concept of the prioritization engine is retrieve predetermined

exposure information associated with the issue, and to prioritize the response activity

utilizing the predetermined exposure information, predetermined exposure information

indicating at east one of a loss and liability value attributed to the issue is well known in

the art as taught by Khanolkar. Khanolar discloses the prioritization engine is retrieve

predetermined exposure information associated with the issue, and to prioritize the

response activity utilizing the predetermined exposure information, predetermined

exposure information indicating at east one of a loss and liability value attributed to the

issue. (Pg. 3 [0035] Event manager 55 processes the event object, calculating it

according to pre-determined criteria, which may be based on the type of the event, and

assigns a severity level. Based on security level, event manager 55 filters the event

object, thereby determining accordingly whether the event object is to be broadcast

and/or to be saved). Criteria are based on type of events such as intrusions. It would

have been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include the prioritization engine is retrieve predetermined exposure information

associated with the issue, and to prioritize the response activity utilizing the

predetermined exposure information, predetermined exposure information indicating at

east one of a loss and liability value attributed to the issue in order to have a user –

friendly technique with which specify quality of service requirements for each host, each

application, and the network in which the hosts are connected.


As per claim 20 Witter and Masters discloses all the limitations of claim 20 which are

described above. Witter did not disclose wherein the performance data indicates a

historical accuracy with which the reporting entity has previously reported issues

pertaining to the system. The general concept of wherein the performance data

indicates a historical accuracy with which the reporting entity has previously reported

issues pertaining to the system is well known in the art as taught by Khanolkar.

Khanolkar discloses wherein the performance data indicates a historical accuracy with

which the reporting entity has previously reported issues pertaining to the system

(Khanolkar:  Pg. 1 [0004] Presented with log data, however, monitoring devices often

fail in two respects. First, they fail to effectively monitor log data from all relevant

components on the network. Second, they fail to record and report the log data in a form

that is timely and useful to network administrators. Moreover, while various systems

such as firewalls and intrusion detection systems, such as NetRanger from Cisco

Systems, Inc., may issue real time alarms to a network administrator of an intrusion

event based on log data; within a network such alarms may be lost in the midst of

numerous notices of intrusion events received by a network administrator. What is

needed is a system to process and organize network intrusion events and log data from

a number of network systems and provide them to a user in an interface that

summarizes them, yet has links to more detailed information, that provides for real time

notice and communications regarding current events, and that allows for the compilation

and recalling of past log data and intrusion events for detection of patterns of activity for

later use and consultation). It would have been obvious to one of ordinary skill in the art

at the time of the invention to modify Witter in order to include wherein the performance

data indicates a historical accuracy with which the reporting entity has previously

reported issues pertaining to the system in order to provide access to the corresponding

event object information via an alarm console.


As per claim 21 Witter and Masters discloses all the limitations of claim 21 which are

described above. Witter did not disclose wherein the historical accuracy is expressed in

terms of a number of false positive issue data received from the reporting entity. The

general concept of wherein the historical accuracy is expressed in terms of a number of

false positive issue data received from the reporting entity is well known in the art as

taught by Khanolkar. Khanolkar discloses the historical accuracy is expressed in terms

of a number of false positive issue data i.e. event object received from the reporting

entity (Khanolar: Each event object that is created is read, and the intrusion event

information it contains is assigned a severity level. Event objects meeting or exceeding

a predetermined threshold security level, or other threshold criteria, may be broadcast

to the user and displayed as an intrusion alarm on a user interface display screen in real

time. Users may set filters regulating the stream of event objects received as

broadcasts based on severity level or other criteria or may choose to receive all event

objects regardless of severity or other criteria as broadcast intrusion alarms). It would

have been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include the historical accuracy is expressed in terms of a number of false

positive issue data received from the reporting entity in order to provide access to the

corresponding event object information via an alarm console.

As per claim 22 Witter and Masters discloses all the limitations of claim 22 which are

described above. Witter did not disclose wherein the performance data a rate at which

the reporting entity has previously reported issues pertaining to the system. The general

concept of the performance data indicates a rate at which the reporting entity has

previously reported issues pertaining to the system is well known in the art as taught by

Khanolakor. Khanolakor discloses the performance data indicates a rate at which the

reporting entity has previously reported issues pertaining to the system (Khanolakor:

Pg. 1 [0006] In response to an intrusion event, the security monitoring system can issue

intrusion alarms to network administrative users ("users"), who will then be able to

obtain information regarding intrusion events in real time on a display screen. The

system filters log data, which contains information related to intrusion events, to provide

a more manageable flow of data that can be more easily reviewed by a system

administrator because the data relating to intrusion events are not "lost" in large

amounts of noise (e.g., data not relating to intrusion events). The system has means for

organizing and collating intrusion event data within a searchable database accessible to

a user through a reporting system that can generate security reports and summaries of

intrusion events for network service devices and that provides information in response

to user queries). It would have been obvious to one of ordinary skill in the art at the time

of the invention to modify Witter to include the performance data indicates a rate at

which the reporting entity has previously reported issues pertaining to the system in

order to provide access to the corresponding event object information via an alarm

console.


As per claim 23 Witter and Masters discloses all the limitations of claim 23 which are

described above. Witter did not disclose assessing the validity of the issue pertaining to

the system as reported in the issue data, and updating the performance data regarding

the reporting entity based on the assessed validity of the issue The general concept of

the user performance module is to assess validity of the issue pertaining to the system

as reported in the issue data, and to update the performance data regarding the

reporting entity based on the assessed validity of the issue is well known in the art as

taught by Khanolakor. Khanolakor discloses the user performance module is to assess

validity of the issue pertaining to the system as reported in the issue data, and to update

the performance data regarding the reporting entity based on the assessed validity of

the issue (Pg. 1 [0008] Each event object that is created is read, and the intrusion event

information it contains is assigned a severity level. Event objects meeting or exceeding

a predetermined threshold security level, or other threshold criteria, may be broadcast

to the user and displayed as an intrusion alarm on a user interface display screen in real

time. Users may set filters regulating the stream of event objects received as

broadcasts based on severity level or other criteria or may choose to receive all event

objects regardless of severity or other criteria as broadcast intrusion alarms). It would

have been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include the user performance module is to assess validity of the issue

pertaining to the system as reported in the issue data, and to update the performance

data regarding the reporting entity based on the assessed validity of the issue in order

to provide access to the corresponding event object information via an alarm console.


As per claim 24 Witter and Masters discloses all the limitations of claim 24 which are

described above. Witter did not disclose the updating if the performance data includes

registering at least one of a false positive and a false negative with respect to the issue.

The general concept of the user performance module is to update the performance data by registering at least one of a false positive and a false negative with respect issue is well known in the art as taught by Khanolakar. Khanolar discloses the user performance module is to update the performance data by registering at least one of a false positive and a false negative with respect issue (Pg. 3 [0004] Logging is the procedure by which operating systems record events in the system as they happen. Within the logging memory of these devices, and other devices such as web servers, e-mail servers, DNS servers, etc., logs are kept that contain data comprising information chronicling network intrusion events. Presented with log data, however, monitoring devices often fail in two respects. First, they fail to effectively monitor log data from all relevant components on the network. Second, they fail to record and report the log data in a form that is timely and useful to network administrators. Moreover, while various systems such as firewalls and intrusion detection systems, such as NetRanger from Cisco Systems, Inc., may issue real time alarms to a network administrator of an intrusion event based on log data; within a network such alarms may be lost in the midst of numerous notices of intrusion events received by a network administrator. What is needed is a system to process and organize network intrusion events and log data from a number of network systems and provide them to a user in an interface that summarizes them, yet has links to more detailed information, that provides for real time notice and communications regarding current events, and that allows for the compilation and recalling of past log data and intrusion events for detection of patterns of activity for later use and consultation). It would have been obvious to one of ordinary skill in the art at the time of

the invention to modify Witter in order to provide access to the corresponding event

object information via an alarm console.

As per claim 31 Witter and Masters discloses all the limitation of claim 31 which is

described above. Witter did not discloses retrieving predetermined exposure information

associated with the issue, and prioritizing the response activity utilizing the

predetermined exposure information, the predetermined exposure information indicating

at least one of a loss and liability value attributed to the issue. The general concept of

the prioritization engine is retrieve predetermined exposure information associated with

the issue, and to prioritize the response activity utilizing the predetermined exposure

information, predetermined exposure information indicating at east one of a loss and

liability value attributed to the issue is well known in the art as taught by Khanolkar.

Khanolar discloses the prioritization engine is retrieve predetermined exposure

information associated with the issue, and to prioritize the response activity utilizing the

predetermined exposure information, predetermined exposure information indicating at

east one of a loss and liability value attributed to the issue. (Pg. 3 [0035] Event manager

55 processes the event object, calculating it according to pre-determined criteria, which

may be based on the type of the event, and assigns a severity level. Based on security

level, event manager 55 filters the event object, thereby determining accordingly

whether the event object is to be broadcast and/or to be saved). Criteria are based on

type of events such as intrusions. It would have been obvious to one of ordinary skill in

the art at the time of the invention to modify Witter to include the prioritization engine is

retrieve predetermined exposure information associated with the issue, and to prioritize

the response activity utilizing the predetermined exposure information, predetermined

exposure information indicating at east one of a loss and liability value attributed to the

issue in order to have a user –friendly technique with which specify quality of service

requirements for each host, each application, and the network in which the hosts are

connected.

Claims 9,27, are rejected under 35 U.S.C. 103 (a) as being unpatentable over Witter

(US 2003/0208497 A1) in view of Masters (US 7,051,098 B2) further in view of Kaplan

(US 7,155,510 B1).

As per claim 9 Witter and Masters discloses all the limitations of claim 9 which is

described above. Witter did not discloses wherein the agent is an automated agent and

a human agent. The general concept of wherein the agent is an automated agent and a

human agent is well known in the art as taught by Kaplan. Kaplan discloses the agent is

an automated agent and a human agent (Col.4 lines 38-52). It would have been obvious

to one of ordinary skill in the art at the time of the invention to modify Witter to include

the agent is an automated agent and a human agent in order to provide.

As per claim 27 Witter and Masters discloses all the limitations of claim 27 which is described above. Witter did not disclose wherein the agent is at least one of an automated agent and a human agent. The general concept of wherein the agent is at least one of an automated agent and a human agent is well known in the art as taught by Kaplan. Kaplan discloses wherein the agent is at least one of an automated agent and a human agent (Col.4 lines 38-52). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Witter to include the agent is at least one of an automated agent and a human agent in order to provide

Claims 10,14,28 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Witter (US 2003/0208497 A1) in view of Masters (US 7,051,098 B2) further in view of Hashem (US 2003/0041291 A1).

As per claim 10 Witter and Masters discloses all the limitations of claim 10 which is described above. Witter did not disclose wherein the prioritization engine automatically to increment a count value indicative a number of times that the issue, pertaining to the system, has been reported, and to prioritize the response activity utilizing the count value. The general concept of the prioritization engine automatically to increment a count value indicative a number of times that the issue, pertaining to the system, has been reported, and to prioritize the response activity utilizing the count value is well known in the art as taught by Hashem. Hashem discloses the prioritization engine

automatically to increment a count value indicative a number of times that the issue,

pertaining to the system, has been reported, and to prioritize the response activity

utilizing the count value (Pg. 2 [0023], [0024]). It would have been obvious to one of

ordinary skill in the art at the time of the invention to modify Witter to include the

prioritization engine automatically to increment a count value indicative a number of

times that the issue, pertaining to the system, has been reported, and to prioritize the

response activity utilizing the count value in order to efficiently and economically track

errors found in documents formed by an imaging process.

As per claim 14 Witter and Masters discloses all the limitations of claim 10 which is

described above. Witter and Masters also discloses wherein the prioritization engine is

prioritize the response activity utilizing a combination of at least two of the performance

data (Masters; Col. lines 48-62), a predetermined severity value associated with the

issue (Masters; Col. 31 lines 45-55) (Col. 33 lines 60-67), and exposure information

associated with the issue (Witter; Pg. 3 paragraph [0036]). Witter and Master did not

disclose a count of number of times that the issue has been reported. The general

concept of a count of number of times that the issue has been reported is well known in

the art as taught by Hashem. Hashem discloses a count of number of times that the

issue has been reported (Pg.2 [0023], [0024]). It would have been obvious to one of

ordinary skill in the art at the time of the invention to modify Witter to include a count of

number of times that the issue has been reported in order to efficiently and

economically track errors found in documents formed by an imaging process.

As per claim 28 Witter and Masters discloses all the limitations of claim 28 which is described above. Witter did not disclose automatically incrementing a count value indicative a number of times that the issue, pertaining to the system, has been reported, and prioritizing the response activity utilizing the count value. The general concept of automatically incrementing a count value indicative a number of times that the issue, pertaining to the system, has been reported, and prioritizing the response activity utilizing the count value is well known in the art as taught by Hashem. Hashem discloses automatically incrementing a count value indicative a number of times that the issue, pertaining to the system, has been reported, and prioritizing the response activity utilizing the count value (Pg. 2 [0023], [0024]). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Witter to include automatically incrementing a count value indicative a number of times that the issue, pertaining to the system, has been reported, and prioritizing the response activity utilizing the count value in order to efficiently and economically track errors found in documents formed by an imaging process.

Claim 15- 17,33-35 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Witter (US 2003/0208497 A1) in view of Masters (US 7,051,098 B2) further in view of Robinson (US 5,734,838).

As per claim 15 Witter and Masters discloses all the limitations of claim 15 which is described above. Witter did not disclose including an incentive engine to provide an incentive award to the reporting entity. The general concept of including an incentive engine to provide an incentive award to the reporting entity is well known in the art as taught by Robinson. Robinson discloses including an incentive engine to provide an incentive award to the reporting entity (Abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Witter to include an incentive engine to provide an incentive award to the reporting entity in order to create an anchor or foundation for interaction with the customer associated with the administrating institution. In this connection, it is advantageous to provide customers with transaction intensive account services so that the customer will constantly and periodically identify or recognize the administrating institution, which is administering the customer accounts.

As per claim 16 Witter and Masters discloses all the limitations of claim 16 which is described above. Witter did not disclose wherein the incentive award is provided to the reporting entity by the incentive engine responsive to receipt of the issue data. The general concept of the incentive award is provided to the reporting entity by the incentive engine responsive to receipt of the issue data as taught by Robinson. Robinson discloses wherein the incentive award is provided to the reporting entity by the incentive engine responsive to receipt of the issue data (Abstract). It would have

been obvious to one of ordinary skill in the art at the time of the invention to modify

Witter to include the incentive award is provided to the reporting entity by the incentive

engine responsive to receipt of the issue data in order to create an anchor or foundation

for interaction with the customer associated with the administrating institution. In this

connection, it is advantageous to provide customers with transaction intensive account

services so that the customer will constantly and periodically identify or recognize the

administrating institution, which is administering the customer accounts.


As per claim 17 Witter and Masters disclose all the limitations of claim 17 which is

described above. Witter did not disclose the incentive award is provided to the reporting

entity by the incentive engine responsive to the performance data of the reporting entity

satisfying predetermined criteria. The general concept of the incentive award is provided

to the reporting entity by the incentive engine responsive to the performance data of the

reporting entity satisfying predetermined criteria is well known in the art as taught by

Robinson. Robinson discloses the incentive award is provided to the reporting entity by

the incentive engine responsive to the performance data of the reporting entity

satisfying predetermined criteria (Abstract lines 16-25). It would have been obvious to

one of ordinary skill in the art at the time of the invention to modify Robinson to include

the incentive award is provided to the reporting entity by the incentive engine

responsive to the performance data of the reporting entity satisfying predetermined

criteria in order to create an anchor or foundation for interaction with the customer

associated with the administrating institution. In this connection, it is advantageous to

provide customers with transaction intensive account services so that the customer will constantly and periodically identify or recognize the administrating institution, which is administering the customer accounts.

As per claim 33 Witter and Masters discloses all the limitations of claim 33 which is described above. Witter did not disclose providing an incentive award to the reporting entity. The general concept of providing an incentive award to the reporting entity is well known in the art as taught by Robinson. Robinson discloses providing an incentive award to the reporting entity (Abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Witter to include providing an incentive award to the reporting entity in order to create an anchor or foundation for interaction with the customer associated with the administrating institution. In this connection, it is advantageous to provide customers with transaction intensive account services so that the customer will constantly and periodically identify or recognize the administrating institution, which is administering the customer accounts.

As per claim 34 Witter and Masters discloses all the limitations of claim 34 which is described above. Witter did not disclose the incentive award is provided to the reporting entity responsive to receipt of the issue data. The general concept of the incentive award is provided to the reporting entity responsive to receipt of the issue data is well known in the art as taught by Robinson. Robinson discloses the incentive award is provided to the reporting entity responsive to receipt of the issue data (Abstract). It

would have been obvious to one of ordinary skill in the art at the time of the invention to

modify Witter to include the incentive award is provided to the reporting entity

responsive to receipt of the issue data in order to create an anchor or foundation for

interaction with the customer associated with the administrating institution. In this

connection, it is advantageous to provide customers with transaction intensive account

services so that the customer will constantly and periodically identify or recognize the

administrating institution, which is administering the customer accounts.


As per claim 35 Witter and Masters discloses all the limitations of claim 35 which is

described above. Witter did not disclose the incentive award is provided to the reporting

entity responsive to the performance data of the reporting entity satisfying

predetermined criteria. The general concept of the incentive award is provided to the

reporting entity by the incentive engine responsive to the performance data of the

reporting entity satisfying predetermined criteria is well known in the art as taught by

Robinson. Robinson discloses the incentive award is provided to the reporting entity by

the incentive engine responsive to the performance data of the reporting entity

satisfying predetermined criteria (Abstract lines 16-25). It would have been obvious to

one of ordinary skill in the art at the time of the invention to modify Robinson to include

the incentive award is provided to the reporting entity by the incentive engine

responsive to the performance data of the reporting entity satisfying predetermined

criteria in order to create an anchor or foundation for interaction with the customer

associated with the administrating institution. In this connection, it is advantageous to

provide customers with transaction intensive account services so that the customer will

constantly and periodically identify or recognize the administrating institution, which is

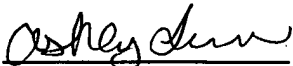administering the customer accounts.

## *Conclusion*

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Ashley d. Turner whose telephone number is 571-270-

1603. The examiner can normally be reached on Monday thru Friday 7:30a.m. -

5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nathan Flynn can be reached at 571-272-1915. The fax phone number for

the organization where this application or proceeding is assigned is 571-270-2603.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

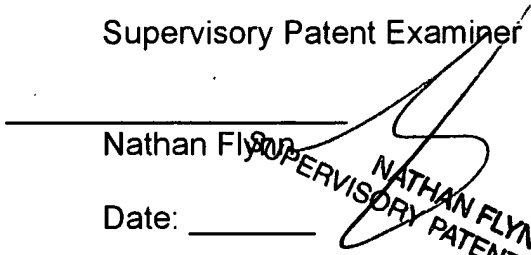system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Patent Examiner:

Ashley Turner
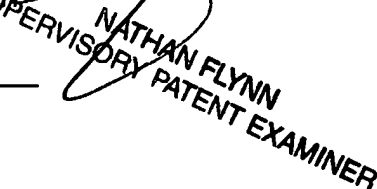
Date: 12/3/2007

Supervisory Patent Examiner

Nathan Flynn

Date: _____